



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/804,835	03/19/2004	Ramarathnam Venkatesan	MSI-1286US	7125
22801	7590	09/14/2007		
LEE & HAYES PLLC 421 W RIVERSIDE AVENUE SUITE 500 SPOKANE, WA 99201			EXAMINER PERUNGAVOOR, VENKATANARAY	
			ART UNIT 2132	PAPER NUMBER
			MAIL DATE 09/14/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

# Office Action Summary

Application No.

10/804,835

Applicant(s)

VENKATESAN ET AL.

Examiner

Venkat Perungavoor

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 19 March 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-37 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-37 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 19 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

## DETAILED ACTION

### *Claim Rejections - 35 USC § 101*

1. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 1-8, 20-27 and 35-37 discloses medium as being a carrier wave which is an non-statutory subject matter.
3. Claims 9-10 produces no tangible result and also related to non-statutory subject matter.

### *Claim Rejections - 35 USC § 102*

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-3, 6-8, 11-15, 18-19, are rejected under 35 U.S.C. 102(b) as being anticipated by NPL to Tsujii.
6. Regarding Claim 1, 13, Tsujii discloses the obtaining message M see Page 467- II. El Gamal's Public-Key Cryptosystem-<Encryption>; defining a vector to  $v_1 \dots v_n$  based upon a predefined first hashing function of the message see Page 468 -(12); calculating a private key  $\alpha$  in accordance with equation  $\sum_{1 \leq i \leq n} v_i \alpha_i \bmod m$  see Page 468 item 16; producing a signature S in accordance with the equation  $S = \alpha H_2(M)$ , where  $H_2(M)$  is a predefined second hashing function see Page 470-(39).

Art Unit: 2132

7. Regarding Claim 2, 11, 14, Tsujii discloses the results of indicating message and signature(M,S) see Page 471-(55).
8. Regarding Claim 3, 15, Tsujii discloses the mapping of third hashing into an integer range see Page 469- Second Column 2- "An arbitrary.."
9. Regarding Claim 6-7, 18-19, Tsujii discloses the hashing in -1 and 1 see Page 469 Second full paragraph "An abitrary..."
10. Regarding Claim 8, 12, Tsujii discloses the output device and medium see Page 471 "Enhancement of Security and Processing Cost".

***Claim Rejections - 35 USC § 103***

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
  - a. A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.
12. Claims 4-5, 9-10, 16-17, 20-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over NPL to Tsujii in view of NPL2 to Chen.
13. Regarding Claim 4-5, 9-10,16-17, 22, 30,Tsujii disclose the discrete logs of points on an elliptic curve and tate-weil pairings. However, Chen discloses the discrete logs of points on

an elliptic curve and tate-weil pairings see Page 9 14¶ “Suppose that there are...”. It would be obvious to one having ordinary skill in the art at the time of the invention to include the discrete logs of points on an elliptic curve and tate-weil pairings in the invention of Tsujii in order to unique session keys.

14. Regarding Claim 20, 27, 28, 35, 37, Tsujii discloses the obtaining message M and signature(M,S) see Page 471-(55) & Page 467- II. El Gamal's Public-Key Cryptosystem- <Encryption>; defining a vector to  $v_1, \dots, v_n$  based upon a predefined first hashing function of the message see Page 468 -(12); calculating a private key  $\alpha$  in accordance with equation  $Q = \sum_{1 \leq i \leq n} v_i Q_i \text{ mod } m$  see Page 468 item 16. But does not disclose the calculating the point on an elliptic curve, comparing of pair (P, S) and pair (Q,  $H_2(M)$ ) and indicating results of comparing. However, Chen discloses the point on an elliptic curve (Page 3 1¶), comparing of pair (P, S) and pair (Q,  $H_2(M)$ ) and indicating results of comparing see (Page 1¶ “At the conclusion...”). It would be obvious to one having ordinary skill in the art at the time of the invention to include the calculating the point on an elliptic curve, comparing of pair (P, S) and pair (Q,  $H_2(M)$ ) and indicating results of comparing in the invention of Tsujii in order to have an authentication system/key verification system as taught in Chen see Page 10 9¶ “The method used ...”.

15. Regarding Claim 21, 29, 36, Tsujii discloses the results of indicating message and signature(M,S) see Page 471-(55).

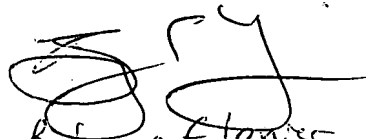
Art Unit: 2132

16. Regarding Claim 23-26, 31-34, Chen discloses the comparing not a match then the repeating the defining, calculating, modifying and comparing see Page 10 7¶ ("The proof...").

*Conclusion*

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkat Perungavoor whose telephone number is 571-272-7213. The examiner can normally be reached on 8:30-5:00. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.
18. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/VP/  
Venkat Perungavoor  
Examiner  
Art Unit 2132  
September 4, 2007

  
Benjamin G. Tanner  
Examiner AU 2132